Lerch Quotients, Lerch Primes, Fermat-Wilson Quotients, and the Wieferich-non-Wilson Primes 2, 3, 14771

Jonathan Sondow
209 West 97th Street, New York, NY 10025
e-mail: jsondow@alumni.princeton.edu

Abstract The Fermat quotient $q_p(a) := (a^{p-1}-1)/p$, for prime $p \nmid a$, and the Wilson quotient $w_p := ((p-1)!+1)/p$ are integers. If $p \mid w_p$, then p is a Wilson prime. For odd p, Lerch proved that $(\sum_{a=1}^{p-1} q_p(a) - w_p)/p$ is also an integer; we call it the *Lerch quotient* ℓ_p. If $p \mid \ell_p$ we say p is a *Lerch prime*. A simple Bernoulli-number test for Lerch primes is proven. There are four Lerch primes $3, 103, 839, 2237$ up to 3×10^6; we relate them to the known Wilson primes $5, 13, 563$. Generalizations are suggested. Next, if p is a non-Wilson prime, then $q_p(w_p)$ is an integer that we call the *Fermat-Wilson quotient* of p. The GCD of all $q_p(w_p)$ is shown to be 24. If $p \mid q_p(a)$, then p is a Wieferich prime base a; we give a survey of them. Taking $a = w_p$, if $p \mid q_p(w_p)$ we say p is a *Wieferich-non-Wilson prime*. There are three up to 10^7, namely, $2, 3, 14771$. Several open problems are discussed.

1 Introduction

By Fermat's little theorem and Wilson's theorem, if p is a prime and a is an integer not divisible by p, then the *Fermat quotient of p base a*,

$$q_p(a) := \frac{a^{p-1}-1}{p}, \tag{1}$$

and the *Wilson quotient of p*,

$$w_p := \frac{(p-1)!+1}{p}, \tag{2}$$

are integers. (See [25, pp. 16 and 19] and [26, pp. 216–217].)

For example, the Fermat quotients of the prime $p = 5$ base $a = 1, 2, 3, 4$ are $q_5(a) = 0, 3, 16, 51$; the Fermat quotients of $p = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$ base $a = 2$ are

$$q_p(2) = \frac{2^{p-1}-1}{p} = 1,3,9,93,315,3855,13797,182361,9256395,34636833,\ldots$$

[28, sequence A007663]; and the Wilson quotients of $p = 2,3,5,7,11,13,17,\ldots$ are

$$w_p = 1,1,5,103,329891,36846277,1230752346353,\ldots$$

[28, sequence A007619].

A prime p is called a *Wilson prime* [15, section A2], [25, p. 277] if p divides w_p, that is, if the supercongruence

$$(p-1)! + 1 \equiv 0 \pmod{p^2}$$

holds. (A *supercongruence* is a congruence whose modulus is a prime power.)

For $p = 2,3,5,7,11,13$, we find that $w_p \equiv 1,1,0,5,1,0 \pmod{p}$ (see [28, sequence A002068]), and so the first two Wilson primes are 5 and 13. The third and largest known one is 563, uncovered by Goldberg [13] in 1953. Crandall, Dilcher, and Pomerance [4] reported in 1997 that there are no new Wilson primes up to 5×10^8.

Vandiver in 1955 famously said (as quoted by MacHale [21, p. 140]):

> It is not known if there are infinitely many Wilson primes. This question seems to be of such a character that if I should come to life any time after my death and some mathematician were to tell me that it had definitely been settled, I think I would immediately drop dead again.

As analogs of Fermat quotients, Wilson quotients, and Wilson primes, we introduce Lerch quotients and Lerch primes in Section 2, and Fermat-Wilson quotients and Wieferich-non-Wilson primes in Section 3. We define them by combining Fermat and Wilson quotients in apparently new ways.

2 Lerch quotients and Lerch primes

In 1905 Lerch [20] proved a congruence relating the Fermat and Wilson quotients of an odd prime.

Lerch's Formula. *If a prime p is odd, then*

$$\sum_{a=1}^{p-1} q_p(a) \equiv w_p \pmod{p},$$

that is,

$$\sum_{a=1}^{p-1} a^{p-1} - p - (p-1)! \equiv 0 \pmod{p^2}. \tag{3}$$

Proof. Replace a with ab in equation (1). Substituting $a^{p-1} = pq_p(a)+1$ and $b^{p-1} = pq_p(b)+1$, we deduce Eisenstein's logarithmic relation [10]

$$q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}$$

and Lerch's formula follows. For details, see [20] or [29]. □

Ribenboim [26, p. 218] explains the point of Lerch's formula this way:

> Since the Fermat quotient is somehow hard to compute, it is more natural to relate their sums, over all the residue classes, to quantities defined by p.

Wilson quotients and Lerch's formula have been used (see [29]) to characterize solutions of the congruence

$$1^n + 2^n + \cdots + k^n \equiv (k+1)^n \pmod{k^2}.$$

2.1 Lerch quotients

Lerch's formula allows us to introduce the Lerch quotient of an odd prime, by analogy with the classical Fermat and Wilson quotients of any prime.

Definition 1. The *Lerch quotient* of an odd prime p is the integer

$$\ell_p := \frac{\sum_{a=1}^{p-1} q_p(a) - w_p}{p} = \frac{\sum_{a=1}^{p-1} a^{p-1} - p - (p-1)!}{p^2}.$$

For instance,

$$\ell_5 = \frac{0+3+16+51-5}{5} = \frac{1+16+81+256-5-24}{25} = 13.$$

The Lerch quotients of $p = 3,5,7,11,13,17,19,23,29,\ldots$ are

$$\begin{aligned}\ell_p = {} & 0, 13, 1356, 123229034, 79417031713, 97237045496594199,\\ & 166710337513971577670, 9930903101797948988080580 68,\\ & 6099522134583881348494451272163714744 9, \ldots,\end{aligned}$$

and for prime $p \le 62563$ the only Lerch quotient ℓ_p that is itself a prime number is $\ell_5 = 13$ (see [28, Sequence A197630]). By contrast, the Wilson quotients w_p of the primes $p = 5,7,11,29,773,1321,2621$ are themselves prime [15, Section A2], [28, Sequence A050299].

2.2 Lerch Primes and Bernoulli Numbers

We define Lerch primes by analogy with Wilson primes.

Definition 2. An odd prime p is a *Lerch prime* if p divides ℓ_p, that is, if

$$\sum_{a=1}^{p-1} a^{p-1} - p - (p-1)! \equiv 0 \pmod{p^3}. \tag{4}$$

For $p = 3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,\ldots$, we find that

$$\begin{aligned}\ell_p \equiv\ & 0,3,5,5,6,12,13,3,7,19,2,21,34,33,52,31,51,38,32,25,25,25,\\ & 53,22,98,0,\ldots \pmod{p}\end{aligned}$$

[28, Sequence A197631], and so the first two Lerch primes are 3 and 103.

We give a test for Lerch primes involving *Bernoulli numbers*. Ubiquitous in number theory, analysis, and topology (see Dilcher [7]), they are rational numbers B_n defined implicitly for $n \geq 1$ by the symbolic recurrence relation

$$(B+1)^{n+1} - B^{n+1} = 0.$$

(Ribenboim [26, p. 218] says, "Treat B as an indeterminate and, after computing the polynomial in the left-hand side, replace B^k by B_k.") Thus for $n = 1$, we have $(B+1)^2 - B^2 = 2B_1 + 1 = 0$, and so $B_1 = -1/2$. Now with $n = 2$, we see that $(B+1)^3 - B^3 = 3B_2 + 3B_1 + 1 = 0$ leads to $B_2 = 1/6$. In this way, we get

$$B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0, B_6 = \frac{1}{42}, B_7 = 0, B_8 = -\frac{1}{30}, B_9 = 0, B_{10} = \frac{5}{66}, \ldots.$$

In 1937 (before the era of high-speed computers!) Emma Lehmer [19] showed that 5 and 13 are the only Wilson primes $p \leq 211$. To do this, she used her husband D. H. Lehmer's table of Bernoulli numbers up to B_{220}, together with *Glaisher's congruence* [11] (see also [20]), which holds for any prime p:

$$w_p \equiv B_{p-1} + \frac{1}{p} - 1 \pmod{p}. \tag{5}$$

Here recall the definition

$$\frac{a}{b} \equiv 0 \pmod{m} \quad \Longleftrightarrow \quad m \mid a, \ \ \mathrm{GCD}(a,b) = 1.$$

For example, that 5 is a Wilson prime, but 7 is not, follows from the congruences

$$w_5 \equiv B_4 + \frac{1}{5} - 1 = -\frac{5}{6} \equiv 0 \pmod 5,$$
$$w_7 \equiv B_6 + \frac{1}{7} - 1 = -\frac{5}{6} \not\equiv 0 \pmod 7.$$

Multiplying Glaisher's congruence by p and substituting $pw_p = (p-1)! + 1$ yields *E. Lehmer's test: A prime p is a Wilson prime if and only if*

$$pB_{p-1} \equiv p - 1 \pmod{p^2}.$$

We provide an analogous test for Lerch primes.

Theorem 1 (Test For Lerch Primes). *A prime $p > 3$ is a Lerch prime if and only if*

$$pB_{p-1} \equiv p + (p-1)! \pmod{p^3}. \tag{6}$$

Proof. We first establish the following *Criterion: an odd prime p is a Lerch prime if and only if*

$$(B+p)^p \equiv p^2 + p! \pmod{p^4}. \tag{7}$$

To see this, recall the classical application of Bernoulli numbers called *Faulhaber's formula* (also known as *Bernoulli's formula*—Knuth [18] has insights on this):

$$1^n + 2^n + \cdots + (k-1)^n = \frac{(B+k)^{n+1} - B^{n+1}}{n+1}. \tag{8}$$

(See Conway and Guy [2, pp. 106–109] for a lucid proof.) Now set $k = p$ and $n = p-1$ in (8). It turns out that $B_p = 0$ (indeed, $B_3 = B_5 = B_7 = B_9 = \cdots = 0$; see [2, p. 109], [16, section 7.9]), and it follows that the congruences (4) and (7) are equivalent. This proves the Criterion.

To prove the Test, note that for any odd positive integer p, the vanishing of B_{2k+1} for $k \geq 1$ implies

$$(B+p)^p = p^p + p \cdot p^{p-1} B_1 + \sum_{k=1}^{(p-1)/2} \binom{p}{2k} p^{p-2k} B_{2k}. \tag{9}$$

The von Staudt-Clausen theorem [2, p. 109], [16, section 7.9], [25, p. 340] says in part that the denominator of B_{2k} is the product of all primes q for which $(q-1) \mid 2k$. (For instance, as $(2-1) \mid 2$ and $(3-1) \mid 2$, the denominator of B_2 is $2 \cdot 3$, agreeing with $B_2 = 1/6$.) Thus, if p is an odd prime, then on the right-hand side of (9) only B_{p-1} has denominator divisible by p. From this we see, for $p \geq 5$, that p^4 divides the numerator of each term except $p^2 B_{p-1}$. (For the $k = (p-3)/2$ term, this uses $p \mid \binom{p}{p-3}$.) Therefore, the congruence

$$(B+p)^p \equiv p^2 B_{p-1} \pmod{p^4} \tag{10}$$

holds for *all* primes $p > 3$. Substituting (10) into Criterion (7) and dividing by p, we arrive at Test (6). □

As a bonus, (10) affords a proof of Glaisher's congruence.

Corollary 1. *The congruence* (5) *holds. Equivalently, if p is* any *prime, then*

$$pB_{p-1} \equiv p + (p-1)! \pmod{p^2}. \tag{11}$$

Proof. To see the equivalence, substitute (2) into (5) and multiply by p. To prove (11), first verify it for $p = 2$ and 3. If $p > 3$, use (3), (8), and the fact that $B_p = 0$ to get $(B+p)^p \equiv p^2 + p! \pmod{p^3}$. Then (10) and division by p yield (11). □

Notice that the congruences (6) and (11) are the same, except that in (6) the modulus is p^3, while in (11) it is p^2. However, one cannot prove Corollary 1 trivially (by reducing (6) modulo p^2 instead of p^3), because (6) holds only for Lerch primes, whereas (11) holds for all primes.

2.3 Computing Lerch primes: a surprising crossover

Let us compare two methods of computing Lerch primes: Definition (4) and Test (6). Both require, essentially, computation modulo p^3. The Test seems simpler, but on the other hand it requires computing B_{p-1} modulo p^2.

To find out which is faster, we used the code

```
If[Mod[Sum[PowerMod[a,p-1,p^3], {a,1,p-1}] - p - (p-1)!, p^3]
   == 0, Print[p]]
```

in a *Mathematica* (version 7.0.0) program for (4), and we used the code

```
If[Mod[Numerator[p*Mod[BernoulliB[p-1],p^2] - p - (p-1)!], p^3]
   == 0, Print[p]]
```

in a program for (6). Here `Mod[a,m]` gives a mod m, `PowerMod[a,b,m]` gives a^b mod m (and is faster than `Mod[a^b,m]`), and `BernoulliB[k]` gives B_k.

Table 1 shows the CPU time (on a MacBook Air computer with OS X 10.6 and 2.13GHz Intel processor) for each program to decide whether p is a Lerch prime.

Note the surprising crossover in the interval $10007 \le p \le 20011$: before it, Test (6) is much faster than Definition (4), but after the interval the reverse is true. Notice also that for $p > 10^4$ the CPU times of (4) grow at about the same rate as p, while those of (6) balloon at more than double that rate.

The programs for (4) and (6) searched up to 10^4 in about 47.3 and 0.6 seconds, respectively, and found the Lerch primes $3, 103, 839$, and 2237 (see [28, Sequence A197632]). There are no others up to 10^6, by the program for (4), which consumed about 160 hours. (To run the program for (6) that far up was not feasible.)

Marek Wolf, using a modification of (4), has computed that there are no Lerch primes in the intervals $1000003 \le p \le 4496113$ and $18816869 \le p \le 18977773$, as

well as $32452867 \leq p \leq 32602373$. His computation took six months of CPU time on a 64-bit AMD Opteron 2700 MHz processor at the cluster [17].

	CPU time in seconds		
p	Definition	vs.	Test
5	0.000052	$>$	0.000040
11	0.000069	$>$	0.000044
101	0.000275	$>$	0.000064
1009	0.002636	$>$	0.000156
10007	0.088889	$>$	0.002733
20011	0.183722	$<$	0.337514
30011	0.294120	$<$	0.816416
100003	1.011050	$<$	10.477100
200003	2.117640	$<$	49.372000
300007	3.574630	$<$	121.383000
1000003	12.647500	$<$	1373.750000

Table 1: Time each of two programs takes to compute whether p is a Lerch prime.

2.4 Generalizations

Euler and Gauss extended Fermat's little theorem and Wilson's theorem, respectively, to congruences with a composite modulus n—see [16, Theorems 71 and 129]. The corresponding generalizations of Fermat and Wilson quotients and Wilson primes are called *Euler quotients* $q_n(a)$, *generalized Wilson quotients* w_n, and *Wilson numbers* $n \mid w_n$ (see [28, sequences A157249 and A157250]). (The w_n are not called "Gauss quotients;" that term appears in the theory of hypergeometric functions.) In 1998 Agoh, Dilcher, and Skula [1, Proposition 2.1] (see also Dobson [8] and Cosgrave and Dilcher [3]) extended Lerch's formula to a congruence between the $q_n(a)$ and w_n.

Armed with these facts, one can define *generalized Lerch quotients* ℓ_n and *Lerch numbers* $n \mid \ell_n$. But that's another story for another time.

2.5 Open Problems

To conclude this section, we pose some open problems.

1. Is $\ell_5 = 13$ the only prime Lerch quotient?

2. Is there a fifth Lerch prime? Are there infinitely many?

Of the 78498 primes $p < 10^6$, only four are Lerch primes. Thus the answer to the next question is clearly yes; the only thing lacking is a proof!

3. Do infinitely many *non*-Lerch primes exist?

As the known Lerch primes $3, 103, 839, 2237$ are distinct from the known Wilson primes $5, 13, 563$, we may ask:

4. Is it possible for a number to be a Lerch prime and a Wilson prime simultaneously?

Denoting the nth prime by p_n, the known Wilson primes are p_3, p_6, p_{103}. The primes among the indices $3, 6, 103$, namely, 3 and 103, are Lerch primes. This leads to the question:

5. If p_n is a Wilson prime and n is prime, must n be a Lerch prime?

The answer to the converse question—if n is a Lerch prime, must p_n be a Wilson prime?—is no: p_{839} and p_{2237} lie strictly between 563 and 5×10^8, where according to [4] there are no Wilson primes.

In connection with Problem 5, compare Davis's "Are there coincidences in mathematics?" [5] and Guy's "The strong law of small numbers" [14].

3 Fermat-Wilson quotients and the WW primes 2, 3, 14771

Suppose that a prime p is not a Wilson prime, so that p does not divide its Wilson quotient w_p. Then in the Fermat quotient $q_p(a)$ of p base a, we may take $a = w_p$.

Definition 3. If p is a non-Wilson prime, then the *Fermat-Wilson quotient of* p is the integer

$$q_p(w_p) = \frac{w_p^{p-1} - 1}{p}.$$

For short we write

$$g_p := q_p(w_p).$$

The first five non-Wilson primes are $2, 3, 7, 11, 17$. Since $w_2 = w_3 = 1$, $w_7 = 103$, and $w_{11} = 329891$, the first four Fermat-Wilson quotients are $g_2 = g_3 = 0$,

$$g_7 = \frac{103^6 - 1}{7} = 170578899504,$$

and

$$\begin{aligned} g_{11} &= \frac{329891^{10} - 1}{11} \\ &= 13877524055806959780989143689893161318527010635207294 00 \end{aligned}$$

[28, Sequence A197633]. The fifth one, g_{17}, is a 193-digit number.

3.1 The GCD of all Fermat-Wilson quotients

We saw that at least one Lerch quotient and seven Wilson quotients are prime numbers. What about Fermat-Wilson quotients?

Theorem 2. *The greatest common divisor of all Fermat-Wilson quotients is* 24. *In particular,* $q_p(w_p)$ *is never prime.*

Proof. The prime factorizations of $q_p(w_p) = g_p$ for $p = 7$ and 11 are

$$g_7 = 2^4 \cdot 3^2 \cdot 13 \cdot 17 \cdot 19 \cdot 79 \cdot 3571$$

and

$$\begin{aligned} g_{11} \;=\; & 2^3 \cdot 3 \cdot 5^2 \cdot 37 \cdot 61 \cdot 71 \cdot 271 \cdot 743 \cdot 2999 \cdot 89671 \cdot 44876831 \\ & \cdot 743417279981 \cdot 7989680529881. \end{aligned}$$

Since $g_2 = g_3 = 0$, we thus have

$$\mathrm{GCD}(g_2, g_3, g_7, g_{11}) = 2^3 \cdot 3 = 24.$$

To complete the proof, we show that 24 divides g_p whenever $p > 3$. Since

$$p w_p = (p-1)! + 1,$$

it is clear that if $p \geq 5$, then $p w_p$, and hence w_p, is not divisible by 2 or 3. As even powers of such numbers are $\equiv 1 \pmod 8$ and $\equiv 1 \pmod 3$, and so $\equiv 1 \pmod{24}$, it follows that $p g_p \; (= w_p^{p-1} - 1)$, and hence g_p, is divisible by 24. □

3.2 Wieferich primes base a

Given an integer a, a prime p is called a *Wieferich prime base a* if the supercongruence

$$a^{p-1} \equiv 1 \pmod{p^2} \tag{12}$$

holds. For instance, 11 is a Wieferich prime base 3, because

$$3^{10} - 1 = 59048 = 11^2 \cdot 488.$$

Paraphrasing Ribenboim [25, p. 264], it should be noted that, contrary to the congruence $a^{p-1} \equiv 1 \pmod p$ which is satisfied by every prime p not dividing a, the Wieferich supercongruence (12) is very rarely satisfied.

When it is, p cannot divide a, and so the Fermat quotient $q_p(a)$ is an integer. In fact, (1) shows that a prime p is a Wieferich prime base a if and only if p does not divide a but does divide $q_p(a)$.

In 1909, while still a graduate student at the University of Münster in Germany, Wieferich created a sensation with a result related to Fermat's Last Theorem: *If $x^p + y^p = z^p$, where p is an odd prime not dividing any of the integers x, y, or z, then p is a Wieferich prime base 2*. One year later, Mirimanoff proved that *p is also a Wieferich prime base 3*. (See [6, pp. 110-111], [26, Chapter 8], and [30, p. 163].)

The only known Wieferich primes base 2 (also simply called *Wieferich primes*) are 1093 and 3511, discovered by Meissner in 1913 and Beeger in 1922, respectively. In 2011 Dorais and Klyve [9] computed that there are no others up to 6.7×10^{15}. It is unknown whether infinitely many exist. (Neither is it known whether there are infinitely many *non*-Wieferich primes base 2. However, Silverman has proved it assuming the *abc*-conjecture—see his pleasantly-written paper [27].) Likewise, only two Wieferich primes base 3 (also known as *Mirimanoff primes*) have been found, namely, 11 and 1006003. The second one was uncovered by Kloss in 1965. An unanswered question is whether it is possible for a number to be a Wieferich prime base 2 and base 3 simultaneously. (See [15, section A3] and [25, pp. 263–276, 333–334].)

For tables of all Wieferich primes p base a with $2 < p < 2^{32}$ and $2 \le a \le 99$, see Montgomery [22].

3.3 The Wieferich-non-Wilson primes 2, 3, 14771

Let us consider Wieferich primes p base a where a is the Wilson quotient of p.

Definition 4. Let p be a non-Wilson prime, so that its Fermat-Wilson quotient $q_p(w_p)$ is an integer. If p divides $q_p(w_p)$—equivalently, if the supercongruence

$$w_p^{p-1} \equiv 1 \pmod{p^2} \tag{13}$$

holds—then p is a Wieferich prime base w_p, by definition (12). In that case, we call p a *Wieferich-non-Wilson prime*, or *WW prime* for short.

For the non-Wilson primes $p = 2, 3, 7, 11, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, \ldots$, the Fermat-Wilson quotients $q_p(w_p) = g_p$ are congruent modulo p to

$$g_p \equiv 0, 0, 6, 7, 9, 7, 1, 6, 18, 17, 30, 11, 25, 30, 24, 46, 64, 16, 18, 4, 29, \ldots \pmod{p}$$

[28, Sequence A197634]. In particular, 2 and 3 are WW primes. But they are trivially so, because g_2 and g_3 are *equal* to zero.

Is there a "non-trivial" WW prime? Perhaps surprisingly, the answer is yes but the smallest one is 14771. In the next subsection, we give some details on using a computer to show that 14771 is a WW prime. It is "non-trivial" because $g_{14771} \neq 0$. In fact, taking logarithms, one finds that

$$g_{14771} = \frac{\left(\frac{14770!+1}{14771}\right)^{14770} - 1}{14771} > 10^{8\times 10^8},$$

so that the number g_{14771} has more than 800 million decimal digits.

3.4 Computer search

To search for WW primes, one can use a computer to calculate whether or not a given prime p satisfies condition (13). Explicitly, if the number

$$\left(\frac{(p-1)!+1}{p}\right)^{p-1} \bmod p^2 \tag{14}$$

is equal to 1, then p is a WW prime.

Mathematica's function Mod$[a,m]$ can compute (14) when p is small. But if p is large, an "Overflow" message results. However, it is easy to see that in (14) one may replace $(p-1)!$ with $(p-1)! \bmod p^3$, a much smaller number.

For example, it takes just a few seconds for a program using the code

```
If[PowerMod[(Mod[(p-1)!, p^3] + 1)/p, p-1, p^2] == 1, Print[p]]
```

to test the first 2000 primes and print the WW primes $2, 3, 14771$ (see [28, Sequence A197635]).

Michael Mossinghoff, employing the GMP library [12], has computed that there are no other WW primes up to 10^7.

3.5 More open problems

We conclude with three more open problems.

6. Can one prove that 14771 is a WW prime (i.e., that 14771 divides g_{14771}) without using a computer?

Such a proof would be analogous to those given by Landau and Beeger that 1093 and 3511, respectively, are Wieferich primes base 2. (See Theorem 91 and the notes on Chapter VI in [16], and "History and search status" in [31].) However, proofs for Wieferich primes are comparatively easy, because (high) powers are easy to calculate in modular arithmetic, whereas factorials are unlikely to be calculable in logarithmic time.

7. Is there a fourth WW prime? Are there infinitely many?

Comments similar to those preceding Problem 3 also apply to the next question.

8. Do infinitely many *non*-WW primes exist?

Is it possible to solve Problem 3 or Problem 8 assuming the *abc*-conjecture? (See the remark in Section 3.2 about Silverman's proof.)

Acknowledgments

I am grateful to Wadim Zudilin for suggestions on the Test, for a simplification in computing WW primes, and for verifying that there are no new ones up to 30000, using PARI/GP [23]. I thank Marek Wolf for computing Lerch primes, and Michael Mossinghoff for computing WW primes.

References

1. Agoh, T., Dilcher, K., Skula, L.: Wilson quotients for composite moduli. Math. Comp. **67**, 843–861 (1998)
2. Conway, J.H., Guy, R.K.: The Book of Numbers. Springer-Verlag, New York (1996)
3. Cosgrave, J.B., Dilcher, K.: Extensions of the Gauss-Wilson theorem. Integers **8**, article A39 (2008)
4. Crandall, R., Dilcher, K., Pomerance, C.: A search for Wieferich and Wilson primes. Math. Comp. **66**, 433–449 (1997)
5. Davis, P.J.: Are there coincidences in mathematics? Am. Math. Mon. **88**, 311–320 (1981)
6. Dickson, L.E.: History of the Theory of Numbers, vol. 1. Carnegie Institution of Washington, Washington, D. C. (1919); reprinted by Dover, Mineola, NY (2005)
7. Dilcher, K.: A bibliography of Bernoulli numbers (2011); available at http://www.mscs.dal.ca/~dilcher/bernoulli.html
8. Dobson, J.B.: On Lerch's formula for the Fermat quotient (2012, preprint); available at http://arxiv.org/abs/1103.3907
9. Dorais, F.G., Klyve, D.W.: A Wieferich prime search up to 6.7×10^{15}. J. Integer Seq. **14**, Article 11.9.2 (2011); available at http://www.cs.uwaterloo.ca/journals/JIS/VOL14/Klyve/klyve3.html
10. Eisenstein, F.: Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhaengen und durch gewisse lineare Funktional-Gleichungen definiert werden, Verhandlungen der Koenigl. Preuss. Akademie der Wiss. zu Berlin (1850), 36–42; reprinted in Mathematische Werke, vol. 2, 705–711. Chelsea, New York (1975)
11. Glaisher, J.W.L.: A congruence theorem relating to Eulerian numbers and other coefficients. Proc. Lond. Math. Soc. **32**, 171–198 (1900)
12. GMP: The GNU Multiple Precision Arithmetic Library (2011); available at http://gmplib.org/
13. Goldberg, K.: A table of Wilson quotients and the third Wilson prime. J. Lond. Math. Soc. **28**, 252–256 (1953)
14. Guy, R.K.: The strong law of small numbers. Am. Math. Mon. **95**, 697–712 (1988)
15. Guy, R.K.: Unsolved Problems in Number Theory, 3rd ed. Springer, New York (2004)
16. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 5th ed. Oxford University Press, Oxford (1989)
17. Klaster Instytutu Fizyki Teoretycznej UWr (2012); http://zero.ift.uni.wroc.pl/
18. Knuth, D.: Johann Faulhaber and sums of powers. Math. Comp. **61**, 277–294 (1993)
19. Lehmer, E.: A note on Wilson's quotient. Am. Math. Mon. **44**, 237–238 (1937)
20. Lerch, M.: Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$. Math. Ann. **60**, 471–490 (1905)

21. MacHale, D.: Comic Sections: The Book of Mathematical Jokes, Humour, Wit and Wisdom. Boole Press, Dublin (1993)
22. Montgomery, P.L.: New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$. Math. Comp. **61**, 361–363 (1993)
23. PARI/GP (2011); available at http://pari.math.u-bordeaux.fr/
24. Ribenboim, P.: 1093. Math. Intelligencer **5**, 28–34 (1983)
25. Ribenboim, P.: The Book of Prime Number Records, 2nd. ed. Springer-Verlag, New York (1989)
26. Ribenboim, P.: My Numbers, My Friends: Popular Lectures on Number Theory. Springer-Verlag, New York (2000)
27. Silverman, J.H.: Wieferich's criterion and the *abc*-conjecture. J. Number Theory **30** (2), 226–237 (1988)
28. Sloane, N.J.A.: The On-Line Encyclopedia of Integer Sequences (2011); published at http://oeis.org/
29. Sondow, J., MacMillan, K.: Reducing the Erdős-Moser equation $1^n + 2^n + \cdots + k^n = (k+1)^n$ modulo k and k^2. Integers **11**, article A34 (2011); expanded version available at http://arxiv.org/abs/1011.2154v1
30. Wells, D.: The Penguin Dictionary of Curious and Interesting Numbers. Penguin Books, London (1986)
31. Wikipedia: Wieferich prime (2012); http://en.wikipedia.org/wiki/Wieferich_prime